

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of validating a public key in an elliptic curve cryptosystem using an elliptic curve over a finite field, the public key consisting of two coordinates (x, y) where x and y are elements of said finite field, said method comprising the steps of:
 - a) receiving a public key;
 - b) computing a function of the public key, the function having for each order a predefined value for points of that order; and
 - c) comparing the result of the function to predetermined information to indicate the validity of the public key.
2. A method according to claim 1 further comprising the step of partially validating said public key.
3. A method according to claim 2 wherein said elliptic curve has cofactor 2, said finite field is a binary field, and said function is an algebraic expression.
4. A method according to claim 3 wherein said algebraic expression is the trace of said coordinate x and said predetermined value is 1.
5. A method according to claim 4 wherein the evaluating said trace comprises evaluating a dot product of said coordinate x with a predetermined vector.
6. A method according to claim 1 wherein said elliptic curve has cofactor 4 and said finite field is a binary field with odd exponent, said function is an algebraic expression, said predetermined information is 0 and said method further comprises:
 - a) evaluating a trace of the x-coordinate,
 - b) confirming that said trace is zero,
 - c) confirming that said x-coordinate is not zero.
7. A method according to claim 6 wherein evaluating said trace includes evaluating a dot product of x with a predetermined vector.
8. A method according to claim 7 wherein said algebraic expression is $\text{Tr}(x\text{Hf}(b/x^2))$.

9. A method according to claim 8 wherein evaluating said algebraic expression comprises the steps of:
 - a) finding the square of the x-coordinate;
 - b) finding the ratio of the second coefficient of said elliptic curve with said square;
 - c) finding the half-trace of said ratio;
 - d) finding the product of said half-trace with said x-coordinate;
 - e) finding the trace of said product.
10. A method according to claim 9 wherein evaluating said trace of said product and said trace of said x-coordinate comprises evaluating a dot product of x with a predetermined vector.
11. A method according to claim 9 wherein evaluating said half-trace includes evaluating the matrix product of x with a predetermined matrix.
12. A method according to claim 11 wherein evaluating said trace of said product and said of said x-coordinate includes evaluating a dot product of x with a predetermined vector.
13. A method of validating a point on an elliptic curve defined over a finite field and with order an odd prime times a power of two comprising the steps of:
 - a) partially validating said point,
 - b) attempting to halve said point repeatedly until
 - i. no half is found, or
 - ii. the number of times said point is halved is the exponent of two in said power of two;
 - c) accepting said point if said point is partially valid and said number of times is equal to said exponent.
14. A method of validating a point on an elliptic curve with a known cofactor, comprising the steps of:
 - a) determining factors of said cofactor;
 - b) determining the possibility of scalar division of said point by each of said factors;
 - c) rejecting said point if any of said scalar divisions is not possible.

15. A method according to claim 14 wherein said possibility is determined by determining if a polynomial related to the division polynomial corresponding to said factor has a root.
16. A method of nearly fully validating a point on an elliptic curve with a given cofactor comprising the steps of:
 - a) partially validating said point;
 - b) finding the scalar multiple of said point to said cofactor;
 - c) accepting said point if said point is partially valid and said scalar multiple is the zero element of said elliptic curve.
17. A method of nearly fully validating a point on an elliptic curve with a known cofactor comprising the steps of:
 - a) partially validating said point;
 - b) confirming that said point does not equal each member of a set of predetermined points.
18. A method according to claim 17 wherein said set of predetermined points is the set of points with order dividing said cofactor.